AMENDMENTS TO THE CLAIMS

This listing of Claims shall replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A processor with secure cryptographic capabilities, said processor comprising:

a digital secret ~~comprising~~ including a secret key used in a key-based cryptographic process, wherein ~~said~~ the digital secret is stored only within ~~said~~ the processor, and wherein ~~said~~ the digital secret is operable to be used exclusively by ~~said~~ the processor for both encryption and decryption;

a cryptography engine for performing ~~said~~ the key-based cryptographic process internally within ~~said~~ the processor, ~~said~~ wherein the cryptography engine ~~operable~~ is configured to access ~~said~~ the digital secret; and

internal memory coupled to ~~said~~ the cryptography engine ~~for supporting said~~ and configured to support the key-based cryptographic process, wherein ~~said~~ the internal memory is further ~~for storing~~ configured to store data associated with ~~said~~ the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein ~~said~~ the data is accessible only within ~~said~~ the processor.

2. (Currently Amended) The processor of Claim 1 further comprising an internal bus ~~for facilitating~~ configured to facilitate secure communication between

~~said~~ the cryptography engine, ~~said~~ the digital secret, and ~~said~~ the internal memory within said processor.

3. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the digital secret is securely confined within ~~said~~ the processor.

4. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the internal memory ~~comprises~~ includes microcode for implementing ~~said~~ the key-based cryptographic process on ~~said~~ the data within ~~said~~ the processor, and wherein ~~said~~ the internal memory is ~~operable~~ configured to perform state tracking associated with ~~said~~ the key-based cryptographic process.

5. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the data ~~comprises~~ includes intermediate data generated by ~~said~~ the key-based cryptographic process.

6. (Currently Amended) The processor of Claim 1[[,]] further comprising:

a cryptography unit ~~comprising~~ including a functional unit within ~~said~~ the processor for securely executing ~~said~~ the key-based cryptographic process internally within ~~said~~ the processor, wherein ~~said~~ the cryptography unit ~~comprises~~ includes:

~~said~~ the digital secret;

~~said~~ the cryptography engine; and

~~said~~ the internal memory.

7. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the key-based cryptographic process ~~comprises~~ includes:

a key-based encryption process; and

a key-based decryption process.

8. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the processor ~~comprises~~ includes:

a secure hardware environment ~~providing~~ configured to provide core processing functionality; and

a secure software environment coupled to ~~said~~ the secure hardware environment, ~~said~~ wherein the secure software environment ~~generating~~ is configured to generate executable instructions that are sent to ~~said~~ the secure hardware environment for processing, ~~said~~ wherein the secure hardware environment in combination with ~~said~~ the secure software environment ~~providing~~ is configured to provide processor capability, and wherein ~~said~~ the secure hardware environment is accessible only through ~~said~~ the secure software environment.

9. (Currently Amended) The processor of Claim 1, wherein ~~said~~ the digital secret is unique to ~~said~~ the processor and is permanently and physically manifested within ~~said~~ the processor.

10. (Currently Amended) A processor with cryptographic capabilities, said processor comprising:

a secure cryptography unit, wherein ~~said~~ the cryptography unit is configured to internally ~~provides~~ provide secure cryptographic capabilities as a functional unit within ~~said~~ the processor, ~~said~~ the cryptography unit ~~comprising~~ including:

a cryptography engine ~~for performing~~ configured to perform a key-based cryptographic process;

a digital secret exclusively accessible to ~~said~~ the cryptography engine, wherein ~~said~~ the digital secret ~~comprises~~ includes a secret key used in ~~said~~ the key-based cryptographic process, and wherein ~~said~~ the secret key is ~~operable~~ configured to be used exclusively by ~~said~~ the processor for both encryption and decryption; and

internal memory coupled to ~~said~~ the cryptography engine ~~for supporting said~~ and configured to support the key-based cryptographic process, wherein ~~said~~ the internal memory is further ~~for storing~~ configured to store data associated with ~~said~~ the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein ~~said~~ the data is accessible only within ~~said~~ the processor.

11. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the key-based cryptographic process ~~comprises~~ includes:

a key-based encryption process; and

a key-based decryption process.

12. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the processor ~~comprises~~ is a very long instruction word (VLIW) processor.

13. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the processor ~~comprises~~ includes:

a secure hardware environment providing core processing functionality; and

a secure software environment coupled to ~~said~~ the secure hardware environment, ~~said~~ wherein the secure software environment ~~generating~~ is configured to generate executable instructions that are sent to ~~said~~ the secure hardware environment for processing, ~~said~~ wherein the secure hardware environment in combination with ~~said~~ the secure software environment ~~providing~~ is configured to provide processor capability, and wherein ~~said~~ the secure hardware environment is accessible only through ~~said~~ the secure software environment.

14. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the digital secret is unique to ~~said~~ the processor and is permanently and physically manifested within ~~said~~ the processor.

15. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the digital secret ~~comprises~~ includes:

a plurality of fusible links configured to manifest ~~said~~ the digital secret by permanently setting a binary state in each of ~~said~~ the plurality of fusible links.

16. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the digital secret ~~comprises~~ is calculated using ~~a random number that is generated from~~ an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of ~~said IC chip~~ the processor.

17. (Currently Amended) The processor of Claim 16, wherein ~~said~~ the testing data ~~comprises~~ includes:

wafer test data; and

die test data.

18. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the secure cryptography unit ~~comprises~~ is a fully integrated circuit within ~~said~~ the processor.

19. (Currently Amended) The processor Claim 10, wherein ~~said~~ the digital secret and ~~said~~ the internal memory are fully integrated with ~~said~~ the cryptography engine to facilitate communication without use of a bus.

20. (Currently Amended) The processor of Claim 10, wherein ~~said~~ the key-based cryptography process ~~comprises~~ includes a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptography process.

21. (Currently Amended) A processor with secure cryptographic capabilities, ~~said~~ the processor comprising:

a secure hardware environment ~~providing~~ configured to provide core processing functionality, wherein ~~said~~ the secure hardware environment ~~comprises~~ includes:

a secure cryptography unit ~~for providing~~ configured to provide secure cryptographic capabilities as a functional unit within ~~said~~ the secure hardware environment, wherein ~~said~~ the secure cryptography unit is ~~operable~~ configured to facilitate performance of a key-based cryptographic process performed exclusively by ~~said~~ the processor, wherein ~~said~~ the key-based cryptographic process ~~comprises~~ includes encryption using a digital secret and decryption using ~~said~~ the digital secret, ~~and~~ wherein ~~said~~ the key-based cryptographic process further ~~comprises accessing~~ includes generating data, ~~said~~ wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within ~~said~~ the processor.

22. (Currently Amended) The processor of Claim 21[[,]] further comprising:

a secure software environment ~~for accessing said~~ configured to access the secure hardware environment, ~~said~~ wherein the secure software environment ~~generating~~ is configured to generate executable instructions that are sent to ~~said~~ the secure hardware environment for processing, ~~said~~ wherein the secure hardware environment in combination with ~~said~~ the secure software environment ~~providing~~ is configured to provide processor capability.

23. (Currently Amended) The processor of Claim 21, wherein ~~said~~ the secure cryptography unit ~~comprises~~ includes:

a cryptography engine ~~for performing said~~ configured to perform the key-based cryptographic process;

~~said~~ the digital secret accessible exclusively to ~~said~~ the cryptography engine, wherein ~~said~~ the digital secret ~~comprises~~ includes a secret key used in ~~said~~ the key-based cryptographic process; and

internal memory coupled to ~~said~~ the cryptography engine ~~for supporting said~~ , wherein the internal memory is configured to support the key-based cryptographic process and ~~for performing~~ further configured to perform state tracking associated with ~~said~~ the key-based cryptographic process.

24. (Currently Amended) The processor of Claim 23, wherein ~~said~~ the internal memory is ~~operable~~ configured to securely store ~~said~~ the data, and wherein ~~said~~ the data ~~comprises~~ includes intermediate data generated by ~~said~~ the key-based cryptographic process.

25. (Currently Amended) The processor of Claim 21, wherein ~~said~~ the secure cryptography unit ~~comprises~~ is a fully integrated circuit within ~~said~~ the processor.

26. (Currently Amended) The processor of Claim 23, wherein ~~said~~ the secure cryptography unit ~~comprises~~ is a fully integrated circuit within ~~said~~ the processor, and wherein the secure cryptography unit is configured to facilitate

communication between ~~said~~ the cryptography engine, ~~said~~ the digital secret and ~~said~~ the internal memory without use of a bus.